Annex C
Analysis of Key Corporate Risk 2 – Failure to ensure key governance frameworks are fit for purpose

Background

1. This Annex provides a more detailed analysis of KCR2 – Failure to ensure key governance frameworks are fit for purpose.

2. The description of this risk is as follows: With the current scale and pace of transformation taking place throughout the organisation it is now more important than ever that the council ensures that its key governance frameworks are strong particularly those around statutory compliance including information governance and transparency.

Risk Detail

<u>Increased interactions in relation to FOIA and transparency, and failures to adhere to statutory timescales for responses</u>

3. In an increasingly digital world, there is a continuing and escalating risk that requests for information through the Freedom of Information Act (including Subject Access Requests), the Environmental Information Regulations, and the Local Government Transparency Code will increase. Increasing quantities of such requests will require commensurately greater resources to ensure that the timescales set for responding to those requests are met.

4. Presently, the timescales for initial responses are set out in legislation; however, the timescales for subsequent responses, particularly to the cases raised by the Information Commissioner's Office, are determined by the ICO. In the last year, the timescale for ICO cases have been reduced from 20 working days to 10 working days, significantly increasing the pressure on staff; this will be discussed further below.

5. There is, however, an associated risk that, due to the increased pressure, the Council will find itself unable to meet the statutory and non-statutory timescales for responding to requests. It is already the case that responding to Subject Access Requests within the statutory timescale is frequently challenging, due to the scope of such requests and the time necessary to collate and redact information.

6. The latter of these risks can give rise to an associated risk of intervention by the ICO or other regulators.

<u>Failure to comply with data protection and privacy legislation</u>

7. This remains the most significant risk for the Council under KCR2. While data protection and privacy legislation has been in force for over 25 years, and Data Protection and information security training is mandatory for all employees of CYC, it is also the case that the majority of data breaches are accidents, arising from human error; cases involving malicious intent are extremely rare.

Annex C
Analysis of Key Corporate Risk 2 – Failure to ensure key governance frameworks are fit for purpose

8. Nevertheless, whether accidental or deliberate, failures in data protection are, and will continue to be, the most significant and enduring risk to the Council. Whilst the most high-profile incidents (both Hackney Council and Redcar and Cleveland Councils were victims of significant ransomware attacks) occurred some time ago (2020), in the period since the beginning of January 2024 there have been at last another ten incidents of either hacking or Dedicated Denial of Service (DDoS), including one which affected CYC (an attack on North Yorkshire Council which compromised information held on behalf of CYC's trading standards team).

9. Other incidents are of significantly lower risk, frequently involving e-mails being sent to the wrong recipient, but they remain by far the most prolific incidents. Each of these may give rise to reputational and financial risks, and the Council may struggle to ensure that other parts of the legislation requirements are done either at all or in a timely way.

<u>Failure to comply with regulator audit or inspection actions</u>

10. Because of the continued risks associated with information governance, the Council's Internal Audit service conducts regular audits of elements of its operations. Similarly, the Council regularly consults with representatives of the ICO to seek guidance or assurance in relation to the Council's ongoing performance under FOI and data protection legislation. The Council is also required to submit annual compliance information to the Biometric and Surveillance Camera Commissioner for its use of CCTV including body-worn cameras; complete the NHS England annual data security and protection toolkit for its use of NHS patient data and systems; and a three yearly inspection audit by the Investigatory Powers Commissioner on its use of covert surveillance,

11. Each of these audits and visits carries actions designed to continually improve, or at the very least maintain, the Council's service; however, each action requires a time commitment which becomes increasingly challenging to meet in the current climate. Failure to adhere to the requirements identified by both Internal Audit and the regulators gives rise not only to the risk of service decline, but also to reputational and financial risks.

<u>Failure to have and adhere to consistent and effective records management based on established standards, codes of practice etc</u>

12. The role of records management in Council operations is crucial. While some records may be safely deleted after a short period of time, some records must be kept for 12 years, some for 75 years, and some need to permanently preserved. It is therefore crucial that suitable records management procedures are adopted and followed.

13. In addition to the above, York is almost unique as a city in having an archive of civic documents which stretches back over 900 years. It is of vital importance that the Council recognises the need to preserve and archive

appropriate documents through its archive arrangement with Explore, to ensure the continuation of that unbroken record.

14. The majority of modern documents are, of course, digital or electronic, and it is therefore incumbent on the Council to ensure it has a suitable digital and electronic document storage and archiving solution, operating to current, internationally-recognised archiving standards for digital continuity and preservation of records.

15. For paper documents, archiving may mean continued storage, or digitisation to archiving standards; in either case, due care must be taken to avoid the degradation of the material. The maintenance of archives is a Council function which is presently discharged by York Explore and Archives; failure to maintain those archives may result in adverse impacts on the accreditation of the archive function.

<u>Increased resource, capacity and workload demands resulting from any or all the above</u>

16. A key risk, both currently and for the future, are the resource implications arising from ensuring that the Council maintains current performance in respect of information and transparency requests, data protection requirements, auditor or inspection actions, and suitable records management and archiving solutions.

17. The service is presently staffed to the minimum to ensure performance does not deteriorate. However, as noted above, as demand grows, and as technical requirements become more challenging, there is a likelihood that the current resourcing will be insufficient for future needs. Unfortunately, the Council's funding position is such that it is unlikely that additional resourcing will become available, placing greater pressure on the service.

18. This gives rise to the risk that any element of the service may fall below desired or required standards, thereby raising the risk of additional complaints, reputational damage, escalating regulator enforcement actions and increased costs to the Council if there are successful individual claims for compensation as a result of breaches of data protection and privacy legislation.

Implications

19. The implications for the Council include:
    - a decline in service standards, openness and transparency, leading to an increase in complaints and enforcement action, including fines or legal action, from regulators;
    - potential legal action, including criminal action, against the Council and/or individuals for knowing and reckless breaches of data protection legislation;
    - reduced or removed ability to use covert surveillance powers;

- potential compensation claims;
- reduced confidence in the Council's service, and reputational damage;
- increased difficulties in dealing with partners, such as the NHS; and
- adverse impact on the availability of documents for future historical and research purposes.

Controls

20. The controls in place include:

Policies and Procedures

21. The Council maintains policies and procedures, the aim of which is to minimise the risks arising from the processing of personal data, together with the secure storage of both personal data and sensitive information held by the Council. In addition, in relation to some specific uses of data, the Council is required to implement defined procedures to ensure the lawfulness of both the processing, and also of subsequent actions taken (see, for example, applications under the Regulation of Investigatory Powers Act 2000).

22. These policies are regularly reviewed and updated, with all-staff communications ensuring the widest possible dissemination of these updates.

23. The purpose of these is to ensure that, wherever possible, the Council has defined procedures for dealing with how data is processed and how to deal with inevitable breaches of these procedures.

Mandatory Training

24. In order to reinforce the importance of adherence to the policies and procedures, training in relation to data protection and information security is mandatory for all staff.

25. In addition, specific training is required for defined roles, such as covert surveillance training in relation to those officers dealing with RIPA applications, and those responding officers dealing with FoI/SAR/EIR requests.

26. Further, to ensure a commonality of understanding, the Members Induction programme covered the Code of Conduct and Declarations of Interest, and training in relation to their roles and responsibilities and awareness of data protection, information security, data breaches, FOI/EIR and covert surveillance/RIPA.

27. The purpose of the mandatory training is to ensure that all staff have a clear understanding of the need for robust and disciplined conduct when dealing with information held by the Council.

Annex C
Analysis of Key Corporate Risk 2 – Failure to ensure key governance frameworks are fit for purpose

28. This training, however, does not eliminate the risk of data breaches; rather, it serves to reduce their likelihood, and helps to provide the Council with a defensible position in relation to regulatory action proposed by the ICO.

IT Systems

29. The need for constantly-updated IT security is well acknowledged in all sectors, and the Council's ICT team has, to date, been successful in ensuring that no Ransomware or DDoS attacks have penetrated our security. However, this is an ongoing battle, with the Council receiving hundreds of 'spam' e-mails daily.

30. In this context, the clear advantage of Council ICT is the security of both the system, and of the servers upon which any data is held on behalf of the Council; unfortunately, that is not the case with data held on servers not tied to the Council, and it is for this reason that all Members are provided with CYC equipment and ICT accounts.

31. Alongside the Council's ICT security, the Council remains committed to transparency, and consequent work is continuing to provide anonymised data through the York Open Data platform, to allow greater public understanding of the Council's operations.

Internal Review and Reporting

32. Data protection and information governance matters remain under constant review, through both officer and Member meetings, to ensure timeliness of responses to issues, and to ensure appropriate oversight.

33. To that end, the Council's Governance, Risk, and Assurance Group (GRAG) holds 6-weekly meetings covering a variety of matters including regular corporate governance and ICT updates covering data protection and information governance matters. These meetings also assist in maintaining a close relationship between relevant officers of the Council, including the Senior Information Risk Owner, the Data Protection Officer, and the Caldicott Guardian.

34. In addition, the Council's Internal Audit service conducts regular reviews into relevant aspects of data protection, information governance and control, information security and physical information security. These reviews provide crucial feedback, ensuring that the Council is in a position to secure its necessary information governance accreditations with outside bodies such as the NHS. This is supplemented by a Vendor security assurance assessment process, which aims to ensure that those the Council do business with have adequate information security.

35. Finally, the Audit and Governance Committee receives regular corporate governance updates which cover data protection and information governance matters.

Annex C
Analysis of Key Corporate Risk 2 – Failure to ensure key governance frameworks are fit for purpose

Publication of Information

36. The Council continues to publish information on both its website and through the York Open Data platform, together with information available through the Council's website and through the Modern.gov system for committee information, together with the requirement under the Freedom of Information Act to maintain a publication scheme, with associated publication of information. In addition, regular reviews are conducted by the Council's Business Intelligence team in order to ensure that the Council adheres to the Local Government (Transparency Requirements) (England) Regulations 2014 and the Local Government Transparency Code 2014.

37. In addition, details of forthcoming Key Decisions can be found on the Council's Forward Plan, and the Council's website contains details of all Officer decisions which require publication under the Openness of Local Government Bodies Regulations 2014.

38. Of necessity, however, the Council does not publish all information it holds. Some is personal and/or sensitive, and it would not therefore be appropriate for it to be placed in the public domain, and some would identify weaknesses in Council systems which malicious actors may seek to exploit. Nevertheless, the Council seeks to ensure that it is as transparent as possible whilst protecting both the rights of individuals and the Council itself.

General Issues

39. As is noted above, the Council places great emphasis on the protection of the rights of data subjects (including the Council itself) and devotes significant human and technical resources to ensuring the security of that information. Nevertheless, the risks covered by KC2 are not ones which can ever be 'managed away' and will continue to represent a risk to the Council for the foreseeable future.

40. Attacks by malicious actors (particularly foreign states and well-organised criminal organisations) are an increasing issue, but the majority of data protection incidents are caused by simple human error; whilst the above measures are designed to minimise those risks, it is impossible eliminate such mistakes – they are perhaps a defining feature of humanity – and consequently data protection and information governance measures will continue to be an important element of Council operations.

Risk Rating

41. The gross risk score is 20 (likelihood probable, impact major). After applying the controls detailed above the net risk score is reduced to 19 (likelihood possible, impact major).